

SAND REPORT

SAND2002-3420

Unlimited Release

Printed November 2002

Sandia Extended Network: Overview of the Design Process

Michael D. Gomez

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94-AL85000.

Approved for public release; further dissemination unlimited.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401

Facsimile: (865)576-5728

E-Mail: reports@adonis.osti.gov

Online ordering: <http://www.doe.gov/bridge>

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847

Facsimile: (703)605-6900

E-Mail: orders@ntis.fedworld.gov

Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND2002-3420
Unlimited Release
Printed November 2002

Sandia Extended Network: Overview of the Design Process

Michael D. Gomez
Telecommunication Operations Department
Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185-0812

Abstract

This report describes the process that will be used to develop and submit for approval designs for the Sandia Extended Network (SXN). The process follows the steps in the Change Management Process used in the Telecommunication Operations Department's quality management system. Those steps are planning, requirements review, detailed design analysis, implementation, verification, and validation. Two companion reports complete a description of the designs to date: *Sandia Extended Network: Design Requirements* and *Sandia Extended Network: Conceptual Design Definition*.

Introduction

This overview report describes the process that will be used to develop and submit for approval detailed designs for the Sandia Extended Network (SXN). It was written for the technical managers in support of technical design reviews, the CIO and IIS Directors responsible for the final approval, and the respective network and service providers responsible for implementing the SXN design.

A companion report, *Sandia Extended Network: Conceptual Design Definition*, presents the options considered for the system design and associated cost estimates for equipment. These design alternatives have been studied, and a decision analysis has been conducted to select a recommendation for a system design. Preliminary staff estimates and preliminary deployment details for the selected design alternative will be developed on the basis of the approved design.

The design for the proposed SXN, as described in *Conceptual Design Definition*, was developed using the methodology of the Telecommunications Operations Department's Change Management Process (CMP), which requires planning, requirements review, detailed design analysis, implementation, verification, and validation. The CMP is the product-realization process used by Telecommunications Operations to thoughtfully create, change or alter network, telephone and wireless services at Sandia National Laboratories. It was followed in developing a design for the SXN, as outlined below. The final three steps in making the SXN a reality are, of course, in the future.

Planning

The SXN Design Team in partnership with the network operations managers at Sandia/NM and Sandia/CA will plan the network changes, allowing them to ensure all appropriate resources are in place to support the development of the SXN. A demarcation zone (DMZ)/SXN deployment plan will be developed to ensure that mechanisms are in place to ensure the goal of implementing the SXN can be reached and that procedures are in place to reverse the changes to the SXN should actions create undesirable side effects on the network. Planning ensures that the affected portion of the user community has been notified of the change and of its potential effect on network connectivity over a given time frame.

Review of Change Requirements

Many types of changes can be made to an enterprise. Designing and implementing the SXN falls under the category “network expansion” because connections are to be added to existing data networks and also because of design and feature enhancements.

Determination of the need or desire for these network changes has been made with the involvement of the network designers and the appropriate customer representatives, in this case representatives from IIS Management. Requirements have been obtained from IIS Management and are outlined in the document *Sandia Extended Network: Design Requirements*.

No single, individually assigned Change Management Ticket (CMT) will be issued to implement the SXN, rather multiple CMTs will be generated as the network develops.

Design Analysis

The work that will go into creating a design for the SXN includes 1) analyzing the requirements, 2) developing the design options for implementation, 3) analyzing the design options, and 4) assessing results of the analysis.

1. Analysis of requirements

Requirements will be analyzed to ensure that the customer’s needs are defined well enough that a complete design can be developed around them and to ensure that the action being requested meets the customer’s business and technical goals. In analyzing the requirements, the design team will consider the following for the SXN:

- Throughput – The throughput of the new equipment
- Response – Performance response time of the SXN
- Mean time between failures (MTBF)
- Recovery time
- Special requirements – This particular design activity is focused on “special requirements and special security requirements” contained in the report *Sandia Extended Network: Design Requirements*. The other requirement areas (throughput, response, etc.) are assumed to be on the same order as the current SRN environment.

2. Development of design options

The solutions the design team has developed to date to satisfy requirements are contained in the report *Sandia Extended Network: Conceptual Design Definition*.

3. Analysis of design options

The design team conducted an analysis of at least two different services designs, five different DMZ designs and several network designs. They were analyzed based upon a) performance assessment, b) cost, c) risk assessment, d) security issues, e) assessment of

design trade-offs, and f) a design review. Based on these assessments, several design trade-offs were made to arrive at optimum design proposals. IIS Management has made a decision on the conceptual design after reviewing the proposed design solutions.

3.a. *Performance Assessment*

Based on customer and system requirements, a determination will be made as to whether the design will adequately meet or exceed the operational/system needs of the customer and whether it will scale to support future requirements for the customer and the Laboratories. Since this is a Level-3 design,¹ formal system analysis and/or modeling and simulation of the proposed design may be required. An inherent risk associated with this issue is the expedience with which this particular design is expected to progress.

Qualification of equipment not previously used in Sandia National Laboratories' environments must be conducted before implementation. Equipment proposed during preliminary design will be qualified using the Telecommunication Operations Department's Design-Development-Evaluation Area and its related guidelines.

3.b *Cost*

The Cyber Security Program Manager will provide funding to cover the costs associated with these design solutions. Long-term costs are identified in the report *Sandia Extended Network: Conceptual Design Definition* so that IIS management can agree upon and commit to them.

3. c *Risk assessment*

Two significant concerns have to be recognized and managed. First is the availability of staff time to deploy this network, given that several key personnel are already oversubscribed. Second, mortgages associated with the additional infrastructure that the new environment requires have yet to be completely defined, and more important, programmed and committed to. Management in 9300 must address and resolve these two issues as the staff continues the design activities.

A prevalent belief appears to exist at Sandia that the physical network wire and equipment infrastructure of the Laboratories is pervasive and complete. The baseline SRN capability is in fact not homogeneous and complete as evidenced by current major initiatives such as the External Communication Infrastructure Modernization project, the Exposed Edge project, and others. The concern here is that a completely homogenous SRN environment has not yet been realized at a time when a new infrastructure, the Sandia eXtended Network (SXN), is being proposed.

SRN vulnerabilities currently exist that have not yet been mitigated due to the staff, budget and infrastructure issues described above. An opportunity exists to mitigate some of these security issues, but that can only be reasonably realized through application of additional staff and budget resources.

Given the magnitude of the risks identified, it is suggested that IIS Management develop a risk-management plan to address these specific issues.

¹ See the Telecommunication Operations Department *Change Management Process*.

3.d *Security issues*

A major component of the design is the inclusion and construction of a “demarcation zone” (DMZ) as described in the report *Sandia Extended Network: Conceptual Design Definition*. The model follows implementations that have been used at several prominent Internet service and search engine providers. It provides for robust service and greatly enhanced security features to front-end the network environments.

3.e *Assessment of design trade-offs*

The *Sandia Extended Network: Design Requirements* report identifies security requirements that the system must meet in order to be compliant with the network and security architecture documents. While performing design trade-off studies, the design team will evaluate the pros and cons of each choice with respect to risk, security, performance, schedule, and cost for the designs developed. Security is a key element considered in the trade-off decisions discussed in the report *Sandia Extended Network: Conceptual Design Definition*.

3.f *Design review*

Design reviews provide an independent look at a developed design and the design assessment activities. Two conceptual design reviews were identified; an initial one with 8900 and 9300 management the week of July 22, 2002, and a final one with the CIO the week of July 25, 2002. These reviews helped assure that the design team performed a thorough design job and did not overlook any important issues. Further design reviews will be conducted at the end of the preliminary, detailed, and final design stages.

Implementation

The implementation team will consist of staff in Departments 8910, 8930, 9327, 9329, 9334 and 9336 with the technical expertise to carry out the design change, including the test plan and back-out plan. When the *Sandia Extended Network: Conceptual Design Definition* report is formally approved, IIS management will identify an Implementation Team Lead to carry out realization of the approved design. The steps in implementation are outlined here.

1. Negotiate start/completion dates and times

Before starting the implementation, the Implementation Team Lead must negotiate with IIS Management when the change is to take place and provide an estimate of how long the change will take. The team needs to consider both the actual implementation of the change as well as the test and back-out plans.

2. Acquire equipment

Equipment and materials required for implementation will be procured through established means only after acceptance qualification of vendor solutions has occurred (see “Performance Assessment” in *Sandia Extended Network: Conceptual Design Definition*). All agreements should include a list of equipment and materials, associated

project/task numbers as required, and where applicable, the CMT numbers to which the equipment and material are associated.

3. Install equipment for the DMZ and SXN

Actual installation of equipment, cabling, power, etc. follows appropriate manufacturer's procedures (located on the Web or in written form in the department 9334 library maintained by Bruce Whittet) and Telecommunication Operations field procedures (available on the Web FileShare system). Only trained staff will be allowed to perform installation.

4. Configure the DMZ and SXN

This step consists of actions taken to properly set up and commission the components to meet the design requirements. It includes installing appropriate cards into a chassis, hardware configuration, and software configurations as specified in the design document (e.g., installation of software issue 3.1.15, Access Control List). Configuration is performed according to manufacturer's guidelines or specific Telecommunication Operations procedures (available on the Web FileShare system).

5. Monitor the DMZ and SXN

Monitoring is required to ensure that system operations are occurring properly. This work is focused on proper equipment functionality and not specifically a given user's functionality. The Enterprise Management System Team will assume responsibility for this function.

Verification

The *configuration will be verified* to allow a second check to assure the devices that constitute this system meet the design requirements. This will include tests by 9300 personnel that the SXN network and services and the DMZ are functioning properly end-to-end. In addition to functionality, verification ensures that the design documents any changes to the design, and records are documented and finalized into appropriate 9300 documentation systems (Visionael, NWIS, ARS, etc.).

Department 9327 will perform *security verification* on the systems that constitute this design. This verification assures the security measures put in place perform the intended actions and meet requirements.

Validation

Validation of service delivery is a check with the customer that system requirements were met. This action will require that the Implementation Team Lead contact the Director of Center 9300 to validate that the system installed meets the requirements and expectations.

The Implementation Team Lead will negotiate the expiration of the validation period with the Director of 9300 before the implementation phase begins. This will ensure that IIS Management has sufficient time to validate operations and indicate any issues to the Implementation Team Lead. It also ensures that problems are associated with the initial installation and are not reported or seen as a new trouble. After the validation period has expired, performance or trouble issues must be submitted through the Trouble Resolution Process.

Distribution

MS 0630	M.J. Murphy, 9600
MS 0803	H.L. Pitts, 9601
MS 0622	D.S. Rarick, 9623 (6)
MS 0629	P.D. Merillat, 9500
MS 0801	A.L. Hale, 9300
MS 0801	M.J. Sjulín, 9330
MS 0801	W.F. Mason, 9320
MS 0806	C.R. Jones, 9322 (6)
MS 0806	C.D. Brown, 9322
MS 0363	C.A. Morgan, 9323
MS 0822	C. Pavlakos, 9326
MS 0813	R.M. Cahoon, 9327 (6)
MS 0805	W.D. Schwartz, 9329 (6)
MS 0805	D.J. Bragg Jr., 9329
MS 0805	M.W. Gutscher, 9329
MS 0812	M.J. Benson, 9334 (6)
MS 0812	M.D. Gomez, 9334 (10)
MS 0806	Len Stans, 9336 (6)
MS 9003	K.E. Washington, 8900
MS 9011	T.J. Toole, 8910
MS 9012	R.D. Gay, 8930
MS 9018	Central Technical Files, 8945-1
MS 0899	Technical Library, 9619 (2)
MS 0612	Review/Approval Desk, 9612 for DOE/OSTI